Contrôle CRL HTTP sur un concentrateur Cisco VPN 3000

Table des matières

Introduction

Ce document décrit comment activer la vérification de la liste de révocation de certificats (CRL) pour les certificats d'autorité de certification (CA) installés dans le concentrateur Cisco VPN 3000 à l'aide du mode HTTP.

Un certificat est normalement censé être valide pendant toute sa période de validité. Toutefois, si un certificat devient invalide en raison de changements de nom, de changements d'association entre le sujet et l'autorité de certification et de compromission de sécurité, l'autorité de certification révoque le certificat. En vertu de la norme X.509, les AC révoquent les certificats en émettant périodiquement une LCR signée, chaque certificat révoqué étant identifié par son numéro de série. L'activation de la vérification de la liste de révocation de certificats signifie que chaque fois que le concentrateur VPN utilise le certificat pour l'authentification, il vérifie également la liste de révocation de certificats pour s'assurer que le certificat en cours de vérification n'a pas été révoqué.

Les autorités de certification utilisent des bases de données LDAP/HTTP (Lightweight Directory Access Protocol) pour stocker et distribuer les listes de révocation de certificats. Ils peuvent également utiliser d'autres moyens, mais le concentrateur VPN dépend de l'accès LDAP/HTTP.

La vérification de la liste de révocation de certificats HTTP est introduite dans le concentrateur VPN version 3.6 ou ultérieure. Cependant, la vérification des listes de révocation de certificats

basée sur LDAP a été introduite dans les versions antérieures de 3.x. Ce document traite uniquement de la vérification des LCR via HTTP.

Remarque : la taille du cache CRL des concentrateurs de la gamme VPN 3000 dépend de la plate-forme et ne peut pas être configurée selon le souhait de l'administrateur.

Conditions préalables

Exigences

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Vous avez correctement établi le tunnel IPsec à partir des clients matériels VPN 3.x en utilisant des certificats pour l'authentification IKE (Internet Key Exchange) (sans vérification de la liste de révocation de certificats activée).
- Votre concentrateur VPN est toujours connecté au serveur AC.
- Si votre serveur AC est connecté à l'interface publique, vous avez ouvert les règles nécessaires dans le filtre public (par défaut).

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Concentrateur VPN 3000 version 4.0.1 C
- Client matériel VPN 3.x
- Serveur d'autorité de certification Microsoft pour la génération de certificats et la vérification des listes de révocation de certificats sur un serveur Windows 2000.

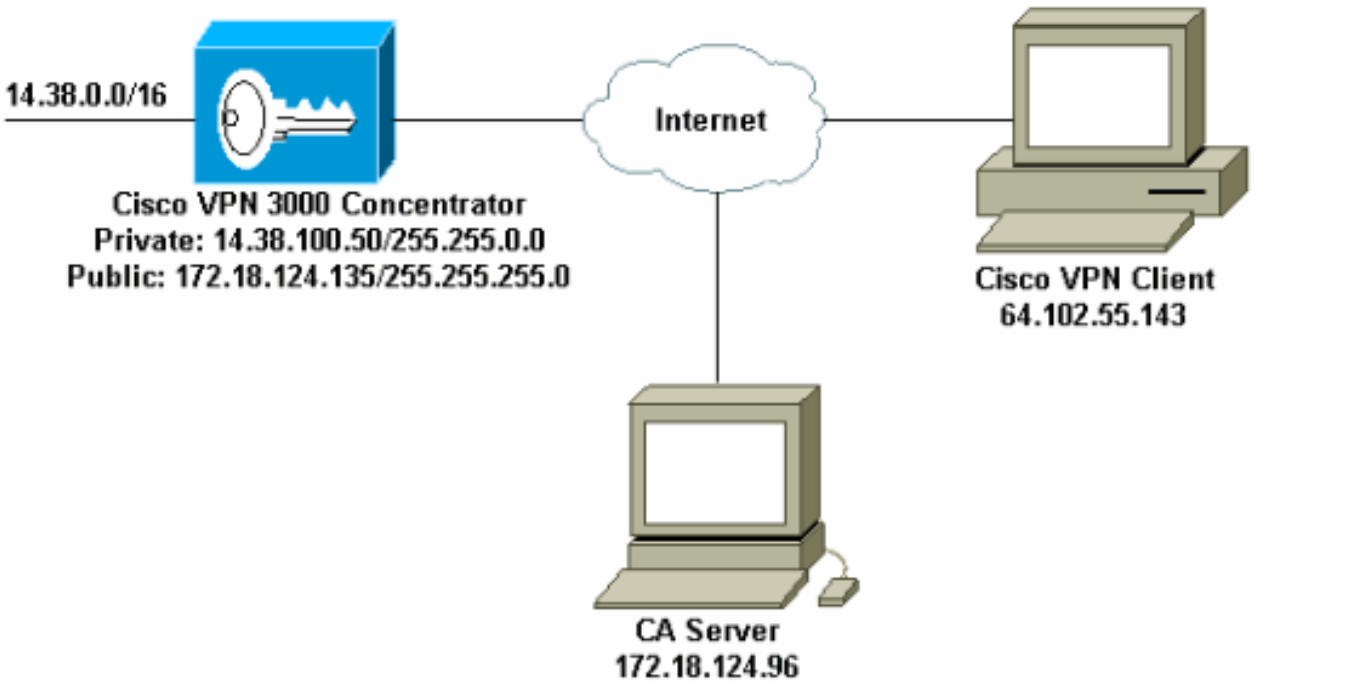
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d’informations sur les conventions utilisées dans ce document, reportez-vous aux Conventions relatives aux conseils techniques Cisco.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



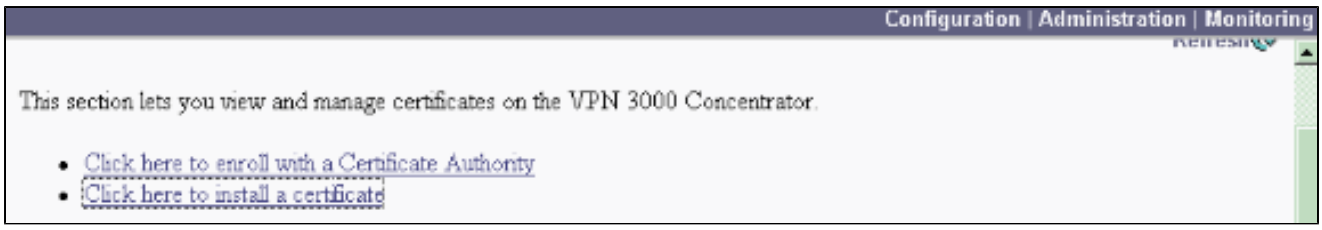
Configuration du concentrateur VPN 3000

Instructions pas à pas

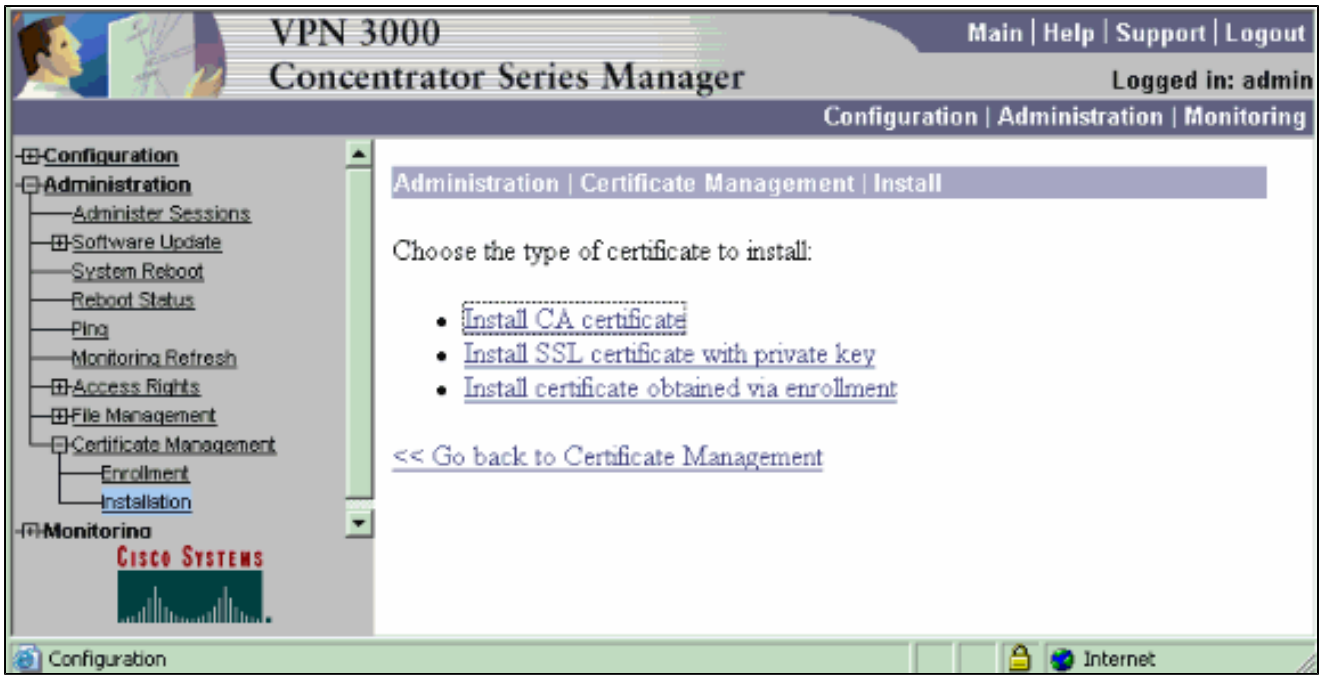
Complétez ces étapes pour configurer le concentrateur VPN 3000 :

1. Sélectionnez Administration > Certificate Management pour demander un certificat si vous n'en avez pas.

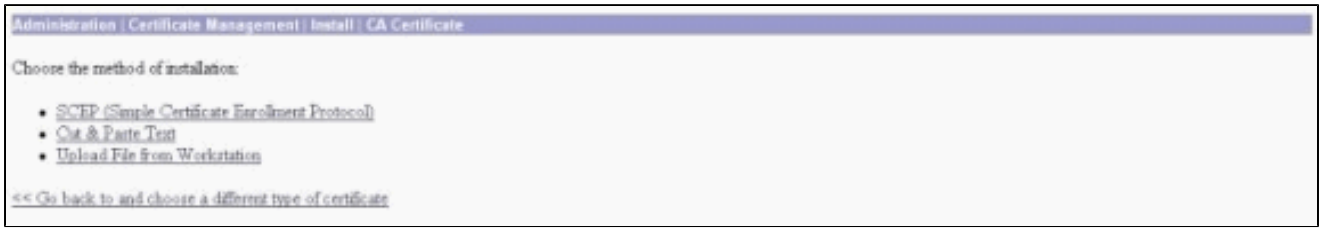
   Sélectionnez Cliquez ici pour installer un certificat pour installer le certificat racine sur le concentrateur VPN.



2. Sélectionnez Installer le certificat CA.

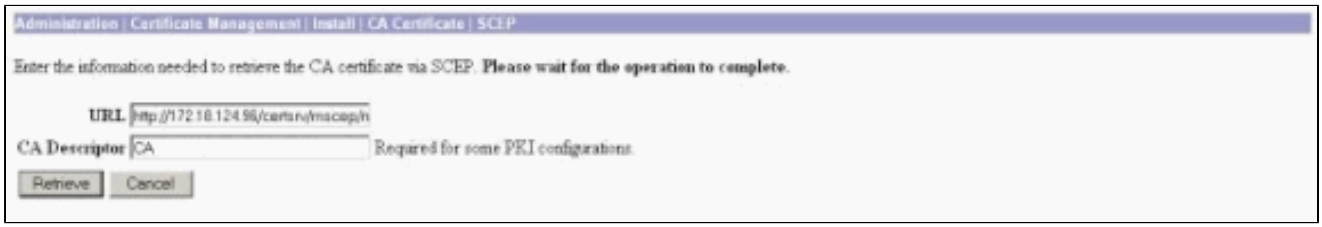


3. Sélectionnez SCEP (Simple Certificate Enrollment Protocol) pour récupérer les certificats d'autorité de certification.



4. Dans la fenêtre SCEP, entrez l'URL complète du serveur AC dans la boîte de dialogue URL.

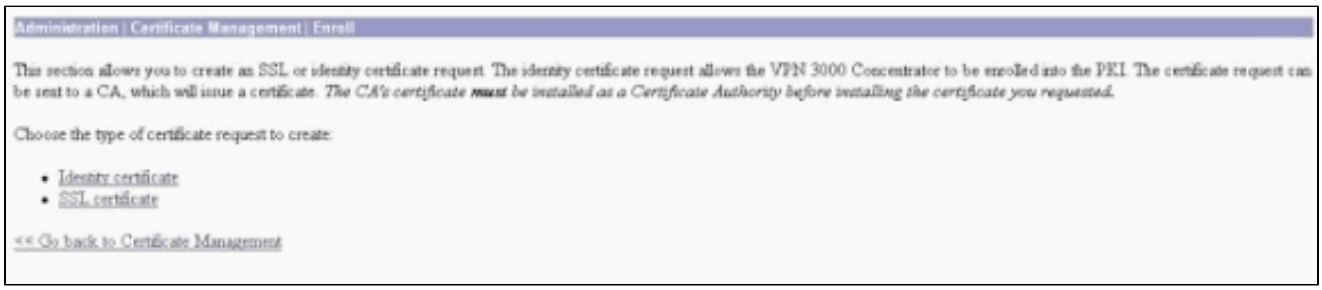
   Dans cet exemple, l'adresse IP du serveur AC est 172.18.124.96. Comme cet exemple utilise le serveur AC de Microsoft, l'URL complète est http://172.18.124.96/certsrv/mscep/mscep.dll. Entrez ensuite un descripteur d'un mot dans la boîte de dialogue Descripteur de l'autorité de certification. Cet exemple utilise CA.



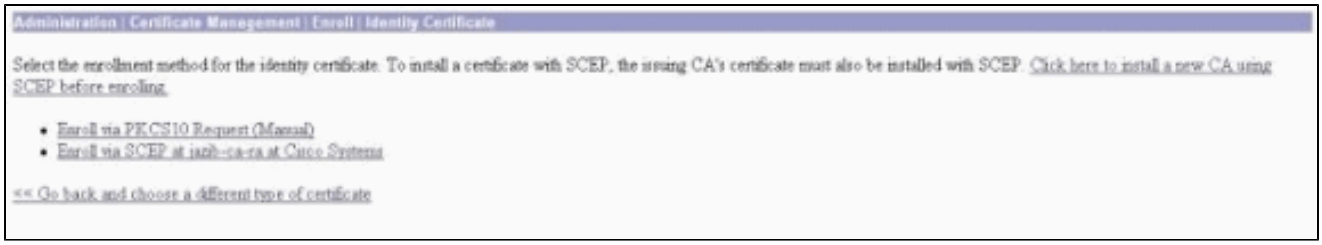
5. Cliquez sur Retrieve.

   Votre certificat CA doit apparaître dans la fenêtre Administration > Certificate Management. Si vous ne voyez pas de certificat, revenez à l'étape 1 et suivez à nouveau la procédure.

6. Une fois que vous avez le certificat CA, sélectionnez Administration > Certificate Management > Enroll, et cliquez sur Identity certificate.



7. Cliquez sur Enroll via SCEP at ... pour demander le certificat d'identité.



8. Complétez ces étapes pour remplir le formulaire d'inscription :

   a. Entrez le nom commun du concentrateur VPN à utiliser dans l'infrastructure à clé publique (PKI) dans le champ Nom commun (CN).

   b. Saisissez votre service dans le champ Unité organisationnelle (OU). L'unité d'organisation doit correspondre au nom de groupe IPsec configuré.

   c. Saisissez votre organisation ou votre société dans le champ Organisation (O).

   d. Saisissez votre ville dans le champ Localité (L).

   e. Saisissez votre état ou votre province dans le champ État/Province (SP).

f. Saisissez votre pays dans le champ Pays (C).

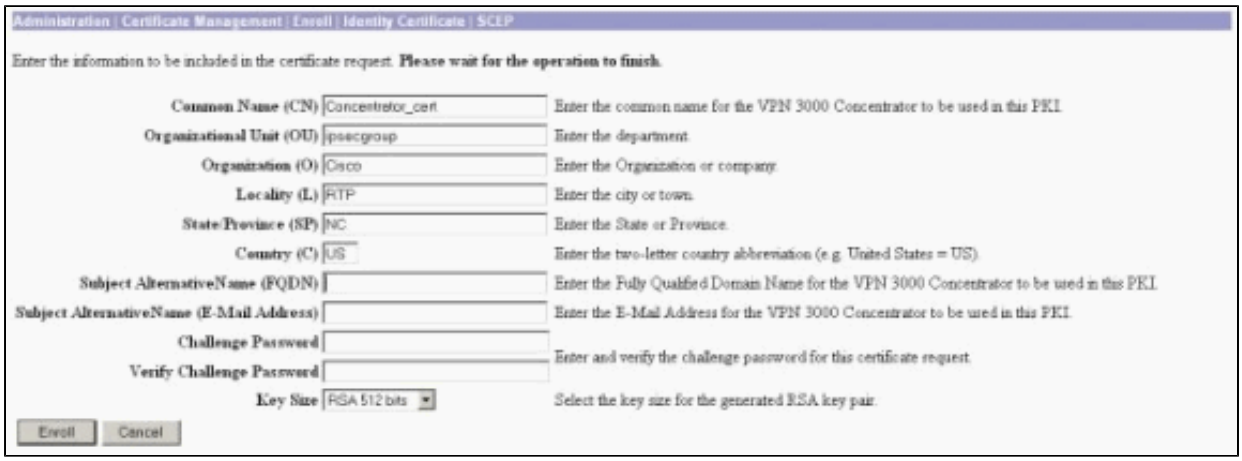
g. Saisissez le nom de domaine complet (FQDN) du concentrateur VPN à utiliser dans l'ICP dans le champ Nom de domaine complet (FQDN).

h. Saisissez l'adresse e-mail du concentrateur VPN à utiliser dans l'ICP dans le champ Subject Alternative Name (email Address).

i. Entrez le mot de passe de demande de certificat dans le champ Mot de passe de demande.

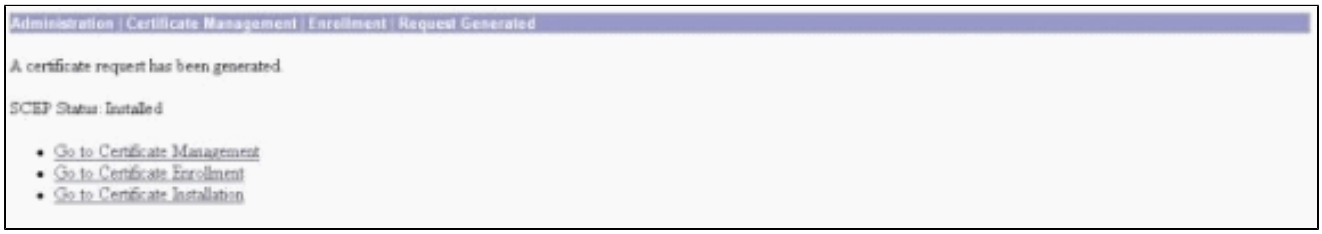
j. Saisissez à nouveau le mot de passe de confirmation dans le champ Vérifier le mot de passe de confirmation.

k. Sélectionnez la taille de clé pour la paire de clés RSA générée dans la liste déroulante Key Size.



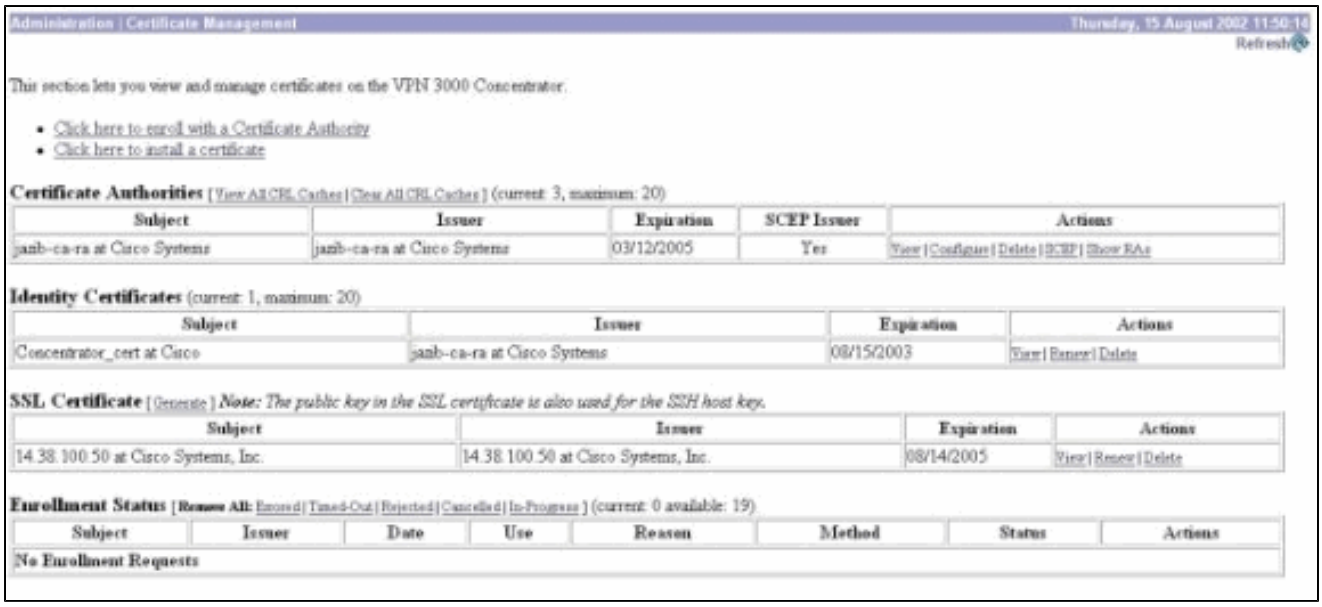
9. Sélectionnez Enroll et affichez l'état SCEP dans l'état d'interrogation.

10. Accédez à votre serveur AC pour approuver le certificat d'identité. Une fois qu'il est approuvé sur le serveur AC, votre état SCEP doit être installé.



11. Sous Certificate Management (Gestion des certificats), votre certificat d'identité doit s'afficher.

    Si ce n'est pas le cas, consultez les journaux sur votre serveur AC pour plus de dépannage.



12. Sélectionnez View sur votre certificat reçu pour voir si votre certificat a un point de distribution CRL (CDP).

    CDP répertorie tous les points de distribution CRL de l'émetteur de ce certificat. Si votre certificat contient le protocole CDP et que vous utilisez un nom DNS pour envoyer une requête au serveur AC, assurez-vous que des serveurs DNS sont définis dans votre concentrateur VPN pour résoudre le nom d'hôte avec une adresse IP. Dans ce cas, le nom d'hôte du serveur AC donné en exemple est jazib-pc, qui correspond à l'adresse IP 172.18.124.96 sur le serveur DNS.

13. Cliquez sur Configure sur votre certificat CA pour activer la vérification CRL sur les certificats reçus.

    Si votre certificat reçu contient le protocole CDP et que vous souhaitez l'utiliser, sélectionnez Utiliser les points de distribution CRL dans le certificat en cours de vérification.

    Étant donné que le système doit récupérer et examiner la liste de révocation de certificats à partir d'un point de distribution réseau, l'activation de la vérification de la liste de révocation de certificats peut ralentir les temps de réponse du système. En outre, si le réseau est lent

ou encombré, la vérification de la liste de révocation de certificats peut échouer. Activez la mise en cache CRL pour limiter ces problèmes potentiels. Cela stocke les listes de révocation de certificats récupérées dans la mémoire volatile locale et permet donc au concentrateur VPN de vérifier plus rapidement l'état de révocation des certificats.

Lorsque la mise en cache de la liste de révocation de certificats est activée, le concentrateur VPN vérifie d'abord si la liste de révocation de certificats requise existe dans le cache et compare le numéro de série du certificat à la liste des numéros de série de la liste de révocation de certificats lorsqu'il doit vérifier l'état de révocation d'un certificat. Le certificat est considéré comme révoqué si son numéro de série est trouvé. Le concentrateur VPN récupère une liste de révocation de certificats à partir d'un serveur externe, soit lorsqu'il ne trouve pas la liste de révocation de certificats requise dans le cache, soit lorsque la période de validité de la liste de révocation de certificats mise en cache a expiré, soit lorsque le temps d'actualisation configuré est écoulé. Lorsque le concentrateur VPN reçoit une nouvelle liste de révocation de certificats d'un serveur externe, il met à jour le cache avec la nouvelle liste de révocation de certificats. Le cache peut contenir jusqu'à 64 listes de révocation de certificats.

Remarque : le cache CRL existe en mémoire. Par conséquent, le redémarrage du concentrateur VPN efface le cache CRL. Le concentrateur VPN remplit à nouveau le cache des listes de révocation de certificats avec des listes de révocation de certificats mises à jour lorsqu'il traite de nouvelles demandes d'authentification homologue.

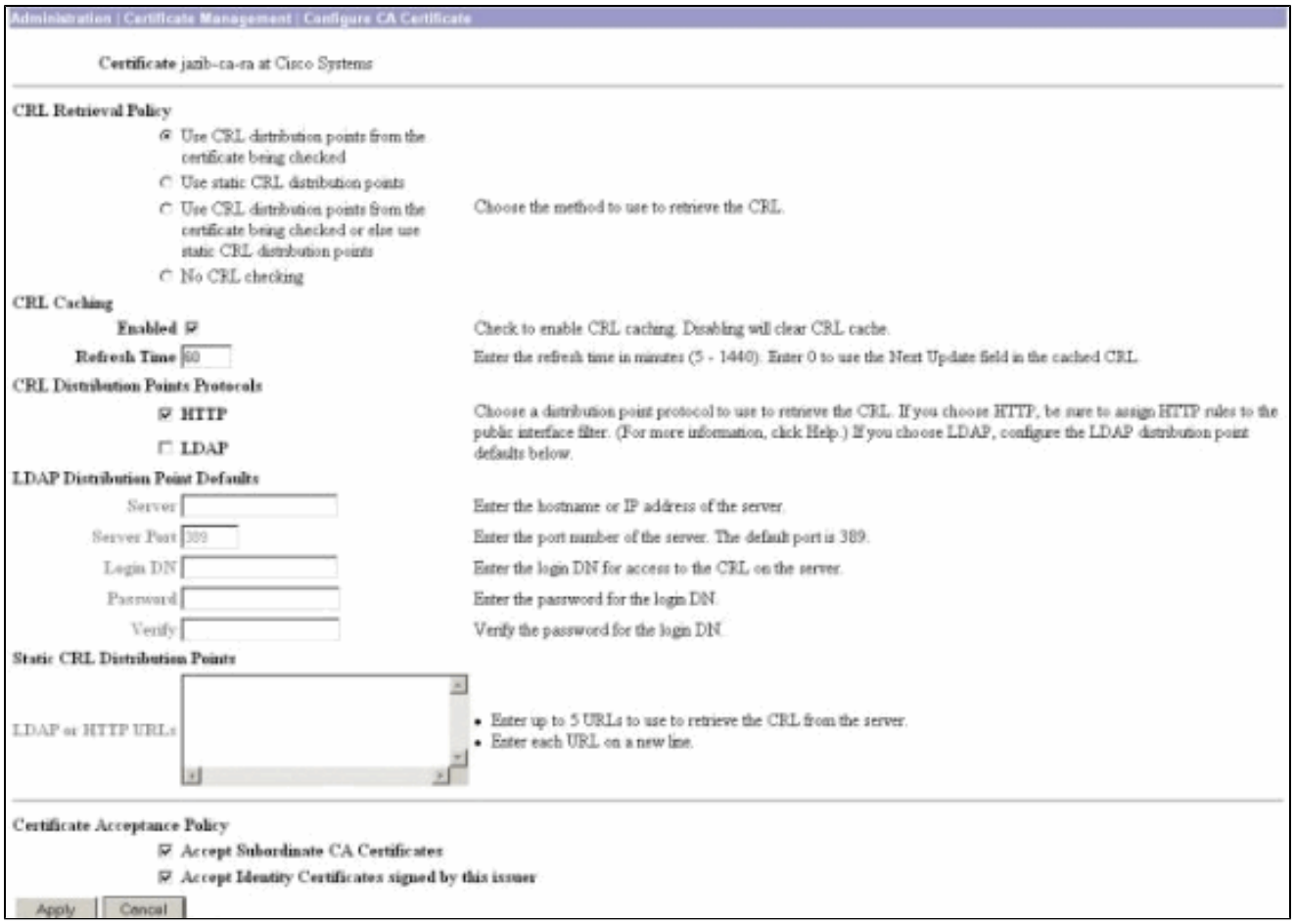
Si vous sélectionnez Utiliser les points de distribution CRL statiques, vous pouvez utiliser jusqu'à cinq points de distribution CRL statiques, comme spécifié dans cette fenêtre. Si vous choisissez cette option, vous devez entrer au moins une URL.

Vous pouvez également sélectionner Utiliser les points de distribution CRL dans le certificat en cours de vérification, ou sélectionner Utiliser les points de distribution CRL statiques. Si le concentrateur VPN ne trouve pas cinq points de distribution CRL dans le certificat, il ajoute des points de distribution CRL statiques, jusqu'à une limite de cinq. Si vous choisissez cette option, activez au moins un protocole de point de distribution CRL. Vous devez également saisir au moins un (et pas plus de cinq) point de distribution CRL statique.

Sélectionnez No CRL Checking si vous souhaitez désactiver la vérification des listes de révocation de certificats.

Sous CRL Caching, cochez la case Enabled pour permettre au concentrateur VPN de mettre en cache les listes de révocation de certificats récupérées. Par défaut, la mise en cache CRL n'est pas activée. Lorsque vous désactivez la mise en cache des listes de révocation de certificats (décochez la case), le cache des listes est effacé.

Si vous avez configuré une stratégie de récupération de liste de révocation de certificats qui utilise des points de distribution de liste de révocation de certificats à partir du certificat vérifié, choisissez un protocole de point de distribution à utiliser pour récupérer la liste de révocation de certificats. Choisissez HTTP dans ce cas pour récupérer la liste de révocation de certificats. Attribuez des règles HTTP au filtre d'interface publique si votre serveur AC est connecté à l'interface publique.



Surveillance

Sélectionnez Administration > Certificate Management et cliquez sur View All CRL caches pour voir si votre concentrateur VPN a mis en cache des CRL à partir du serveur AC.

Vérifier

Cette section fournit des informations qui vous permettront de vérifier que votre configuration fonctionne correctement.

Journaux du concentrateur

Activez ces événements sur le concentrateur VPN afin de vous assurer que la vérification de la liste de révocation de certificats fonctionne.

1. Sélectionnez Configuration > System > Events > Classes pour définir les niveaux de journalisation.
2. Sous Class Name (Nom de classe), sélectionnez IKE, IKEDBG, IPSEC, IPSECDBG ou CERT.
3. Cliquez sur Add ou Modify, et choisissez l'option Severity to Log 1-13.
4. Cliquez sur Apply si vous voulez modifier ou sur Add si vous voulez ajouter une nouvelle

entrée.

Journaux du concentrateur réussis

Si la vérification de votre liste de révocation de certificats réussit, ces messages sont affichés dans les journaux d'événements filtrables.

<#root>

```
1315 08/15/2002 13:11:23.520 SEV=7 CERT/117 RPT=1
The requested CRL was found in cache.
The CRL Distribution point is: http://jazib-pc/CertEnroll/jazib-ca-ra.crl

1317 08/15/2002 13:11:23.520 SEV=8 CERT/46 RPT=1
CERT_CheckCrl(62f56e8, 0, 0)


1318 08/15/2002 13:11:23.520 SEV=7 CERT/2 RPT=1
Certificate has not been revoked: session = 2


1319 08/15/2002 13:11:23.530 SEV=8 CERT/50 RPT=1
CERT_Callback(62f56e8, 0, 0)


1320 08/15/2002 13:11:23.530 SEV=5 IKE/79 RPT=2 64.102.60.53
Group [ipsecgroup]
Validation of certificate successful
(CN=client_cert, SN=61521511000000000086)
```

Reportez-vous à Journaux de concentrateur réussis pour le résultat complet d'un journal de concentrateur réussi.

Journaux défaillants

Si l'archivage de votre liste de révocation de certificats échoue, ces messages s'affichent dans les journaux d'événements filtrables.

<#root>

```
1332 08/15/2002 18:00:36.730 SEV=7 CERT/6 RPT=2
Failed to retrieve revocation list: session = 5


1333 08/15/2002 18:00:36.730 SEV=7 CERT/114 RPT=2
CRL retrieval over HTTP has failed. Please make sure that proper filter rules
have been configured.


1335 08/15/2002 18:00:36.730 SEV=7 CERT/8 RPT=2
Error processing revocation list: session = 5, reason = Failed to retrieve CRL
from the server.
```

Reportez-vous à Revoked Concentrator Logs pour la sortie complète d'un journal de concentrateur défaillant.

Reportez-vous à Journaux des clients réussis pour la sortie complète d'un journal des clients réussi.

Reportez-vous à Revoked Client Logs pour la sortie complète d'un journal client en échec.

Dépannage

Référez-vous à Résolution des problèmes de connexion sur le concentrateur VPN 3000 pour plus d'informations de dépannage.

Informations connexes

- Page de support pour Concentrateurs VPN Cisco 3000
- Page de support pour le Client Cisco VPN 3000
- Négociation IPSec/Protocoles IKE
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.